EXHIBIT E

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,
Plaintiff,

v.

Case No.: 1:22-cv-00187

SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50,
Defendants.

MOOG INC.'S RESPONSES TO DEFENDANT SKYRYSE, INC.'S FIRST SET OF (EXPEDITED) INTERROGATORIES

Pursuant to Federal Rule of Civil Procedure 33, and the March 17, 2022 Stipulation and Order Re: Expedited Discovery (ECF 33, 36), plaintiff Moog Inc. ("Moog") hereby responds and objects to Defendant Skyryse, Inc.'s ("Defendant") Interrogatories ("Interrogatories"). Moog reserves the right to supplement or amend its objections and responses should additional information come to its attention through discovery or otherwise.

PRELIMINARY STATEMENT

These responses are made solely for the purposes of this action. Each response is subject to all objections as to competence, relevance, materiality, propriety and admissibility, and to any and all other objections on any grounds that would require the exclusion of any statements contained in these responses if such a request were asked of, or statements contained in the response were made by, a witness present and testifying in court, all of which objections and grounds are expressly reserved and may be interposed at the time of trial.

Discovery is ongoing and expert reports have not yet been prepared. Accordingly, Moog reserves the right to change, amend or supplement any or all of the matters contained in these responses as additional facts are ascertained, analyses are made, research is completed and contentions are asserted.

Objections to Defendant's First Set of Interrogatories are made on an individual basis below. Moog's response to each Interrogatory is submitted without prejudice to, and without in any way waiving, the General Objections listed below, but not expressly set forth in that response. The assertion of any objection to an Interrogatory in any response below is neither intended as, nor shall in any way be deemed, a waiver of Moog's right to assert that or any other objection at a later date.

GENERAL OBJECTIONS

1. Moog objects that Defendant's First Set of Interrogatories are not consistent with the Federal Rules of Civil Procedure, not warranted by existing law or a good faith argument, interposed for an improper purpose such as to harass Moog and/or cause unnecessary delay and/or needlessly increase the cost of litigation, and is unreasonable, unduly burdensome and expensive.

2. Moog objects to Defendant's First Set of Interrogatories and to each Request on the ground that it is premature and Moog is still in the process of formulating its contentions. Accordingly, Moog reserves the right to amend, supplement or modify its responses to these Requests as further information becomes available and is analyzed by Moog.

3. Moog conducted a diligent search and a reasonable inquiry in a good faith effort to be responsive to Defendant's Interrogatories. As discovery is ongoing, however, Moog reserves the right to make use of, or to introduce at trial, any documents responsive to the

Interrogatories, but discovered subsequent to the date of production, including, but not limited to, any documents obtained in discovery or through further investigation.

4. Moog objects to the Interrogatories to the extent they seek information not reasonably calculated to lead to the discovery of admissible evidence, outside the scope of the Stipulation and Order Re: Expedited Discovery (ECF 33, 36), not relevant to the issues to be decided in Moog's Motion for Preliminary Injunction, or they impose any duty or obligation greater than that provided for in the Federal Rules of Civil Procedure, including Rules 26 and 33, or the Local Rules of the Western District of New York. Moog shall not comply with any purported obligation not imposed by law.

5. Moog objects to the Interrogatories to the extent they seek, or may be interpreted to seek, information protected by the attorney-client privilege, the attorney work product doctrine, and/or any other applicable privilege or restriction on discovery. To the extent that any such information is inadvertently produced, such production shall not waive nor signify intent to waive these respective privileges.

6. Moog objects to the Interrogatories to the extent they seek information or documents already within Defendant's possession, already known or disclosed to Defendant, or which is equally available to Defendant.

7. Moog objects to the Interrogatories to the extent they are vague and ambiguous or so unintelligible that Moog cannot respond.

8. Moog objects to the Interrogatories to the extent they are overbroad. An objection that the Request is "overbroad" means that the Interrogatory seeks, in substantial part,

information or documents that are not relevant to the claim or defense of any party of the pending action or do not appear reasonably calculated to lead to the discovery of admissible evidence.

9. Moog objects to the Interrogatories to the extent they are unduly burdensome. An objection that the Interrogatory is "unduly burdensome" means that the Interrogatory is unreasonably cumulative or duplicative, seeks information or documents that are publicly available or are available from some other source that is more convenient, less burdensome or less expensive, or the burden or expense of the discovery outweighs its benefits.

10. Moog objects to the Interrogatories to the extent they are outside the scope of the Stipulation and Order Re: Expedited Discovery (ECF 33, 36) in furtherance of Moog's Motion for Preliminary Injunction, including but not limited to seeking information regarding allegations and claims that are not used as the basis for Moog's requests for preliminary injunctive relief.

11. Moog objects to the Interrogatories to the extent they seek confidential, proprietary, or sensitive business information, or information otherwise protected by law. Such information, to the extent it is not privileged or otherwise objectionable, will be provided only in accordance with a Stipulated Protective Order granted by the Court and, to the extent necessary, a source code protocol agreed by the parties.

12. Moog objects to the Interrogatories to the extent that they fail to identify the requested information with sufficient specificity to permit a response.

13. In responding to the Interrogatories, Moog does not waive any objections relating to admissibility, relevance, or materiality of any of the information.

14. Moog objects to the definition of "You," "Your," "Plaintiff" or "Moog" contained in Definition No. 1 on the ground that it is broader than permitted by Local Rule 26(c)(3) because it includes "agents . . . affiliates, principals, and/or representatives, individually or collectively, and any other legal entities owned or controlled, directly or indirectly, by any of the foregoing, including attorneys and all persons acting on its behalf or under its control." Moog will use the definition contained in Local Rule 26(c)(3)(E).

15. Moog objects to the definition of "Former Moog Employee" on the grounds that it is vague, ambiguous, and calls for information outside of Moog's possession, custody or control. Moog will construe "Former Moog Employee" to mean any former employee, consultant, or contractor of Moog that Moog knows has become or will become an employee, consultant, or contractor of Skyryse, including the employees identified in paragraph 91 of the Complaint.

16. Moog objects to the definition of "Person" on the grounds that it is broader than permitted by Local Rule 26(c)(3)(F). Moog will use the definition contained in Local Rule 26(c)(3)(F).

17. Moog objects to Definition No. 16 on the grounds that it is broader than permitted by Local Rule 26(c)(3)(F). Moog will use the definition contained in Local Rule 26(c)(3)(F).

18. Moog objects to Definition No. 17 on the grounds that it is broader than permitted by Local Rule 26(c)(3)(E). Moog will use the definition contained in Local Rule 26(c)(3)(E).

19. Moog objects to Definition No. 18 on the grounds that it is broader than permitted by Local Rule 26(c)(3)(C). Moog will use the definition contained in Local Rule 26(c)(3)(C).

20. Moog objects to the "Definitions" and "Instructions" sections of the Interrogatories to the extent they purport to impose discovery burdens on Moog greater than the obligations imposed by the Federal Rules of Civil Procedure and the local rules of the United States District Court for the Western District of New York. Moog will respond and object to the Interrogatories in accordance with the Federal Rules of Civil Procedure and the local rules of the United States District Court for the Western District of New York.

21. Moog objects to Instruction No. 10 on the grounds that the time period of January 1, 2007 to present is overbroad and well beyond the scope of the claims and defenses in the Complaint. Indeed, Defendant was not formed until 2016.

22. Each of the foregoing General Objections is incorporated fully into each individual response that follows. The stating of a specific objection or response shall not be construed as a waiver of Moog's General Objections.

SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES

INTERROGATORY NO. 1:

Identify, for each Defendant, each alleged Trade Secret that You contend that Defendant misappropriated.

RESPONSE TO INTERROGATORY NO. 1:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows: Pursuant to Federal Rule of Civil Procedure 33(d), Moog will make its trade secrets at issue in this case available for inspection by Defendant pursuant to an agreed upon Stipulated Protective Order and source code protocol.

INTERROGATORY NO. 2:

For each alleged Trade Secret identified in response to Interrogatory No. 1, describe in detail how Plaintiff learned of the alleged misappropriation, including, without limitation, the circumstances under which the alleged misappropriation was detected, the identities of the individuals involved in the investigation, the conclusions of any investigation, and the bases for those conclusions.

RESPONSE TO INTERROGATORY NO. 2:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Moog objects to this interrogatory on the grounds that it calls for information or documents protected by the attorney-client privilege, the attorney work product doctrine, and/or any other applicable privilege or restriction on discovery.

Moog objects to this interrogatory on the grounds that it is vague, ambiguous, and compound.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows:

Investigation Involving Ian Bagnald Regarding Kim's Data Theft:

In late January 2022, Katie Kaleta from Moog's IT department reached out to Ian Bagnald (Moog's Security Operations Manager) regarding the then-recent departure of several Moog employees to Skyryse, and asked Bagnald to investigate whether there had been any suspicious activity or copying of data upon these individuals' departures. On January 24, 2022, Bagnald and his team (Philip Horan, Matt Matteson, Shad Northrop, and Keith Barron) began an investigation into the user accounts and data activity associated with these former Moog employees. They took the user names and used a product called Ivanti Device Control, which is an endpoint policy enforcement solution. This software provides endpoint encryption allowing the administrator to enforce certain security policies on removable devices. The program allowed Bagnald to see which files have been downloaded or copied from Moog's internal servers onto removable devices (i.e., external hard drives, USB devices, etc.).

Bagnald's investigation has revealed, among other things, that at least three Moog employees had made copies of Moog data to external devices prior to their exits from Moog. Bagnald's team's analysis has further determined that certain of these employees' copying activities were unsupported by a legitimate business purpose. Bagnald's investigation revealed that Misook Kim ("Kim") had made significant and voluminous data copies that could not be explained from a legitimate business needs standpoint. Ms. Kim worked in Moog's Torrance, California office, along with a number of other software engineers who have recently left Moog's employment to join Skyryse. Ms. Kim's employment with Moog ended December 18, 2021, when she resigned. As part of this investigation, Barron opened the initial case investigation into LogRhythm, Horan and Matteson assisted with the Ivanti Device Control queries related to the investigation, Matteson assisted in gathering certain bitlocker keys, and Northrop helped gathered relevant login events for Misook Kim's user account.

Bagnald's investigation revealed that Ms. Kim had copied 136,994 files to an external hard drive on November 19, 2021, a few weeks before Ms. Kim left Moog's employment. Ms. Kim had taken the hard drive with her after making the copy and after her departure from Moog.

The data Bagnald's investigation has been able to gather from Ms. Kim's electronic devices and Moog user profile include: (1) timestamps of when she used her removable devices; (2) the identifying credentials and specification of the devices that were used in the data copying; and (3) the names and types of the data files that were copied over. Pursuant to Federal Rule of Civil Procedure 33(d), Moog will produce this data on or before April 27, 2022 pursuant to an agreed upon Stipulated Protective Order.

The timestamps for Ms. Kim's user account shows that the unauthorized copying of Moog internal server data to the external hard drive was conducted between November 19, 2021 at 10:16:41 AM UTC and 3:33:28 PM UTC, or between about 3:16 AM to about 7:33 AM local time in California. Our investigation further showed that Ms. Kim copied the data through use of Virtual Private Network ("VPN"), meaning the activity was conducted remotely and outside of direct connection to Moog's servers in Moog's offices.

The specifications for the external hard drive device that Ms. Kim used to extract the data from Moog's internal servers are SAMSUNG PSSD T7 SCSI Disk Device; Model MUPC1T0H; PSID: S9D10DUTM3SS76AGF4193P37BD4NA660; SN: S5SXNS0R702326Z; Capacity: 1 TB.

Based on the information provided by Ian Bagnald's team, Todd Schmidt prepared an Excel spreadsheet with the file log showing the file name and type of each and every file coped by Ms. Kim onto the external hard drive (the "File Log"), included as Exhibit "A" to Ian Bagnald's Declaration (ECF 4-19) which is hereby incorporated by reference. In preparing and analyzing the File Log, Bagnald's team and Schmidt were also able to break down the different file metrics and categories of the 136,994 files copied by Ms. Kim. The overall file metrics are broken down as follows:

- 43,960 source code files;
- 5,377 spreadsheets;
- 2,831 document files;
- 954 executable files;
- 9,003 image files;
- 2,010 MAP files;
- 7,898 model files;
- 1,026 object files;
- 4,613 plain text files;
- 404 presentation files;
- 20,655 miscellaneous files; and
- 38,263 SVN logs.

Bagnald's and his team's investigation of the File Log and underlying data regarding Ms. Kim's data transfer on November 19, 2021 shows that Ms. Kim used Alin Pilkington's file path to copy the data onto the external hard drive. The file path used by Ms. Kim was: "D:\Misook\ENG_Alin_Branch\Software…"

<u>Investigation Involving Mike Hunter and Todd Schmidt Regarding Kim's Data Theft:</u>

Mike Hunter (Senior Software Manager) and Todd Schmidt (Chief Software Engineer) have analyzed the File Log generated by Bagnald and his team. Their review of the File Log showed that the following program classifications were found (showing which program data and code had been copied by Ms. Kim):

- AMP: Actuator Motor Platform. Third iteration of Platform base software for Motors application. Used in both military and commercial programs.

- Sensitive Government Program 1: Military program.
- EHFCAS: Military program.
- eRTOS: Second iteration of Platform base software for Military application. Used in military programs.
- G280: Commercial program.
- Platform: Foundational iteration of Platform base software for commercial purposes. Mostly used on commercial aircraft (G650, G280, C919, 747-8, G7, G8).
- Sensitive Government Program 2: Military program.
- SEPG: A repository of files, internally developed, containing the software process asset library (templates) which guide the software process to be compliant with DO-178 and CMMi.
- Software: Generic files used to aid in the software development process.
- TERN: Military program.
- V280: Military program.
- X47B: Military program.

Their review of the File Log confirmed that the entire source code for Platform was copied by Ms. Kim, meaning that 100% of the base Platform software and its code were copied for at least 2 of the 3 microprocessor applications. All three iterations (commercial, military, motors) of Platform were copied, as well as test artifacts related to some of the iterations. The types of files copied by Ms. Kim for Platform and other software programs and applications include source code, spreadsheets, standalone documents, executables (software executable files including flight programs), images, models (containing pictures or models of functionality), presentations, MAP files (containing variables and addressing of flight code), object files (files created from a compiler containing executable object code—used to link together a flight program), and SVN Logs (files autogenerated from Moog's Subversion network).

In addition to the Platform base software, the data and code for several project-specific applications were also copied, as reflected above. This includes several military programs. The data copied by Ms. Kim includes all of the code, documentation, and related information regarding the composition, testing, and certification of some Platform and project-specific applications. Some projects were copied in their entirety and some projects had select files copied. Ms. Kim copied all 76 of Moog's SEPG checklists as well as other documents from its SEPG repository.

Pilkington, as a former US flight software manager at Moog, was one of a handful of people at Moog (out of thousands) who had access to all Moog flight control artifacts. Kim had similar access because she was one of four administrators of Moog's Subversion repository that houses Moog's software data.

There would be no legitimate reason in Ms. Kim's ordinary job duties for her to attach an external hard drive and copy any data onto it, much less the Platform. The standard way in which Moog employees worked on Platform-related projects would have been to connect to the Moog server and access data that way. If necessary, a copy of the data would be stored to the user's hard drive on their laptop computer – not an external hard drive.

The download by Ms. Kim raised suspicion not only based on the volume of data but also the type of data copied. Ms. Kim was not a development engineer. Her primary job function was software testing. Her knowledge of the platforms, their architectures and the source code files would not be useful to her as a software tester. To perform her testing job functions, she would only need her current program data she is working on, while she was working it. She had no use for the project data after she was completed with that project. That data is specific to a current Moog project.

Even if Ms. Kim wanted to assist with her projects after her departure (as she stated to Jamie Daly in February 2022), she only would have needed to download certain testing data related to the specific project that she was working on, Sensitive Government Project 2. In reference to the File Log, this would have comprised, at most, 0.5% of the total data that Ms. Kim copied. Ms. Kim copied several file classifications, and the entire contents of several programs, that she never had any involvement with. And, Kim's role as a Subversion administrator would have ceased upon leaving Moog.

Investigation Involving Bruce Pixley Regarding Kim's Data Theft:

Bruce W. Pixley, an external expert computer forensic examiner with more than 20 years of experience, was hired to perform an official forensic analysis of true and correct bit-for-bit copies of the Western Digital and Samsung Hard Drives returned by Kim, as well as her two Moog-issued laptop devices ("Dell Laptop 1" and "Dell Laptop 2"). He also reviewed the File Log.

First, Mr. Pixley's analysis determined that Kim had indeed copied 136,994 files of Moog's data on November 19, 2021 between the hours of 3:34 a.m. to 7:33 a.m. PST from Dell Laptop 1 to the Samsung Hard Drive. When Kim copied these files, they were copied to a sub-folder on the Samsung Hard Drive called "Misook."

Second, Mr. Pixley's analysis revealed that "Misook" folder on the same Samsung Hard Drive was intact when it was connected to Dell Laptop 2 on December 15, 2021. On this same date, a new folder was added to the Samsung Hard Drive called "OneNote Notebooks." Microsoft OneNote is a program that is used to store user's notes, drawings, and screen shots. In searching Dell Laptop 2, Mr. Pixley discovered that a folder called “OneNote Notebooks” had been stored in Kim’s Documents folder, containing over 200 digital notebook files. However, on December 17, 2021, Kim’s last day at Moog, the entire “Misook” folder on Dell Laptop 2 was deleted in its entirety. The deleted “Misook” folder contained approximately 54 GB of data. Mr. Pixley’s analysis reveals that this was an intentional user deletion of data and the data was not transferred to the user’s Recycle Bin folder where it could be easily recovered.

The OneNote files contained Kim’s work books created over her years of employment at Moog, and include information helpful to her in utilizing the improperly downloaded data files she took.

Third, and perhaps most importantly, Mr. Pixley’s analysis revealed that the Samsung Hard Drive (which was used to copy 136,994 files on November 19, 2021 and additional notebook data on December 15, 2021) was intentionally formatted sometime after Kim’s departure from Moog on December 17, 2021 and before it was returned on February 21, 2022. When a hard drive is formatted, it needs to be connected to a computer. Mr. Pixley determined that at the start of the formatting process, an option was used that forced the formatting process to overwrite all sectors on the drive with zeroes. Therefore, not only was this formatting of the Samsung Hard Drive an intentional act, but this specific formatting process effectively wiped all previous data on the drive so it would be unrecoverable. This formatting prevents any ability to see the data that was erased on the Samsung Hard Drive. It also prevents any ability to determine whether, when, how, or to where any of the underlying data on the Samsung Hard Drive was copied, transferred, or otherwise exported to another device, or accessed by another party.

Fourth, Mr. Pixley determined that the Samsung Hard Drive had a volume name of "Misook-T7." The volume name for the Western Digital Hard Drive (the initial false hard drive was returned to Moog) had been intentionally changed from its factory default name to "Misook T7," in an apparent attempt to resemble the Samsung Hard Drive that was actually used to copy Moog's data on November 19, 2021 and December 15, 2021.

Mr. Pixley's analysis also revealed that that a ***third*** external hard drive, which has not been located or returned to Moog, was connected to one of Kim's laptops several times in late November 2021.

Finally, an inspection of Kim's two Moog-issued laptop devices indicates that the back covers of the laptops have been removed because the screws were not "factory tight". The laptops' hard drives can be easily accessed and removed by removing the back cover of the laptops.

<u>Investigation Involving Bruce Pixley Regarding Pilkington's Data Theft:</u>

Pixley has additionally conducted an investigation of Pilkington's four Moog-issued laptop devices. With respect to Pilkington's most recent Moog-issued Laptop, Dell Precision 7540, Serial Number 6DDLL33, Hard Drive Serial Number 201030801119 (the "Pilkington Laptop"), Pixley conducted an analysis of the forensic image of the Pilkington Laptop using the following computer forensic software:

- X-Ways version 20.4;
- Forensic Explorer version 5.4.8;
- Axiom version 5.8; and
- Tzworks version 2021.10.10.

Pixley's analysis of the Pilkington Laptop consisted of reviewing file and drive activity and files maintained by the operating system. The operating system files included, but were not limited to, the registry, shortcuts (.lnk files), jumplists, and log files.

Pixley's investigation revealed that on October 27, 2021 (the date that Mr. Pilkington provided notice of his resignation from Moog), Mr. Pilkington copied approximately 1.1 million files of Moog proprietary and confidential data from his Moog-issued laptop onto an external hard drive. Pixley also discovered that on November 12, 2021 (Mr. Pilkington's last day at Moog), he copied approximately 130,000 additional files of Moog proprietary and confidential data from his Moog-issued laptop onto an external hard drive. The external hard drives involved in these acts are: 1) Buffalo 1 TB Hard Drive, USB Serial Number AFDD0200107304; 2) Samsung T7 Thumb Drive, Serial Number S5SCNS0R700159M.

Pixley was able to generate a log and timeline based on the folders and file paths that were copied by Pilkington. This log was provided to Skyryse's counsel via e-mail on April 4, 2022, and is hereby incorporated by reference. A specific file log for each of the approximately 1.2 million files could not be generated from the Pilkington Laptop because the Ivanti software was not functioning properly on the laptop. Regarding the specific sequencing of events as it relates to the Pilkington Laptop, Pixley was able to determine the following:

- 9/9/21 – Pilkington created an account on the Pilkington Laptop.
- 9/10/21 – Pilkington plugs in a Samsung T7 drive (Series T7, serial number S5SXNS0R700159M) (the "Pilkington Samsung T7 Drive") and copies data to the laptop (C:\MoogPrograms).
- 9/11/21 – Pilkington plugs in the Pilkington Samsung T7 Drive and accesses different folders on the drive.

- 9/16/21 - Pilkington plugs in the Pilkington Samsung T7 Drive and accesses different folders on the drive.
- 9/17/21 - Pilkington plugs in the Pilkington Samsung T7 Drive and accesses different folders on the drive.
- 9/21/21 - Pilkington plugs in the Pilkington Samsung T7 Drive and accesses different folders on the drive.
- 9/27/21 - Pilkington plugs in the Pilkington Samsung T7 Drive and copies data to the drive.
- 9/30/21 - Pilkington plugs in the Pilkington Samsung T7 Drive and copies data to the drive.
- 10/27/21 – Pilkington plugs in a Buffalo SSD-PGU3 1 TB external hard drive (the "Buffalo Drive") and copies data to the drive. Pilkington first started copying data at 8:41 a.m. local time. The first folder he created is assigned number 45. The last folder created by Pilkington was 1:49 p.m. local time, and the iNode number is 1,099,360. Therefore, a minimum of 1,000,000 files and folders were copied to the Buffalo Drive during that 5 hour window.
- 11/11/21 – Pilkington plugs in the Pilkington Samsung T7 Drive and copies data to that drive.
- 11/21/21 – Pilkington plugs in the Buffalo Drive and copies data to the drive. Some of the iNode numbers are being reused, suggesting that files were deleted after the initial copy on 10/27/21. New iNode numbers were being assigned (starting with 1,243,139), showing that even more data is being added and it eventually gets up to 1,374,115. Thus, the Buffalo Drive has a minimum of 1,374,115 files and folders on it.

A list of devices that have been imaged by Setec and analyzed by Pixley in connection with his investigation of Pilkington's and Kim's downloads is as follows:

Image	**Custodian**	**Collection Date**	**Make**	**Model**	**Type**	**Serial Number or Service Tag**	**Hard Drive Serial**
#001	Misook Kim	2/24/2022	Western Digital	My Passport	External USB		WX31DB63EDS5
#002	Misook Kim	2/25/2022	Samsung	T7	External USB		S5SXNS0R702326Z
#003	Misook Kim	2/24/2022	Dell	Precision 7540	Computer	9S4Z433	CD03N874710203P6J
#004	Misook Kim	2/25/2022	Dell	Latitude 7480	Computer	FGPYGH2	S415NB0M112161R
#005	Alin Pilkington	3/1/2022	Dell	Precision 7540	Computer	6DDLL33	201030801119
#006	Alin Pilkington	2/25/2022	Dell	Latitude 5591	Computer	BX1KWT2	ED92N039311202J0Y
#007	Alin Pilkington	3/1/2022	Dell	Latitude 7480	Computer	9FWHFH2	S415NB0KA01952D
#008	Alin Pilkington	2/25/2022	Dell	Latitude E6430	Computer	DQ7W3X1	S250NX0H624780T

Investigation Involving Mike Hunter and Todd Schmidt Regarding Pilkington's Data Theft:

Hunter and Schmidt reviewed the timeline and folder log generated by Pixley regarding the Pilkington data theft. Based on their reviews of the copied folder log (the exact files were unavailable due to Pilkington's efforts to cover the evidence of his copying), they determined that the following program classifications were copied:

- 787 (commercial program)
- 747-8 (commercial program)
- A350 (commercial program)
- AMP
- B2 (military program)
- Bullfrog (military program)
- C919 (commercial program)
- Sensitive Government Program 2 (military program)
- EHFCAS (military program)
- Embraer (commercial program)
- Emerald (military program)
- ERTOS
- F15SE (military program)
- F35 (military program)
- F35 (military program)
- G7 (commercial program)
- Platform

- Sensitive Government Program 1 (military program)
- SEPG
- TERN (military program)
- V280 (military program)
- X47B (military program)

Hunter and Schmidt also determined that the largest copy of files occurred from the directory C:\Users\. This is the folder Windows creates for each user on the laptop is all data associated with that user would reside in the sub-folders. This indicates that Pilkington likely copied every file on his computer hard drive outside of the operating system. Hunter and Schmidt also determined there was a large copy (over 200,000 files) of a folder called "MoogPrograms".

Notably, Hunter and Schmidt's analysis revealed that Pilkington copied several different types of data from the various program classifications listed above, including but not limited to source code, system descriptions, specification control drawings, program presentations, software certification documents, hardware certification documents, system models, test cases and test procedures, test results, certification artifacts, tool qualification packages, electrical wiring schematics, actuator and hydraulic schematics, equipment specifications, actuator design and qualification reports, FMEA reports, actuator overhaul manuals, trade secret work instructions, actuator analysis reports, software design artifacts, software design models, electrical interface drawings, mechanical system design description, software verification artifacts, software test cases and procedures, maintainability design requirements, performance models, system models, software verification results, performance analysis documents, electrical schematics, software verification automation tools, and COTS test tools. Pilkington also copied proposal data and cost estimating templates prepared for several of Moog's actual or prospective customers.

Hunter and Schmidt's analysis also determined that there was no legitimate business purpose for the volume and content of the data copied by Pilkington. As a threshold matter, at the time of his departure from Moog, Pilkington was only working on Sensitive Government Programs 1 and 2. If Pilkington felt he had any need to consult or work on Moog projects after his departure, the data he would have needed access to is limited to Sensitive Government Programs 1 and 2. Further, Pilkington never worked on several programs during his time at Moog that he copied data from, including 787, 747-8, A350, AMP, B2, Embraer, F35, Platform, and X47B. Some of these programs are quite old and pre-date Pilkington's employment at Moog. So, data for these programs would not be useful or relevant to any of Pilkington's job functions and duties in connection with Sensitive Government Programs 1 and 2. Finally, Pilkington copied several types of data classifications that were completely unrelated to his job duties as a software engineer, including but not limited to specification control drawings, program presentations, hardware certification documents, electrical wiring schematics, actuator and hydraulic schematics, equipment specifications, actuator design and qualification reports, actuator overhaul manuals, actuator analysis reports, electrical interface drawings, mechanical system design description, maintainability design requirements, electrical schematics, and proposal data and cost estimating templates prepared for several of Moog's actual or prospective customers.

Moog incorporates by reference to this interrogatory response the statements set forth in the Complaint, its Motion for Preliminary Injunction, and the Declarations of Ian Bagnald, Michael Hunter, Todd Schmidt, Jorge Lopez, Jamie Daly, Mike Johnnie and Bruce Pixley filed concurrently therewith.

INTERROGATORY NO. 3:

For each alleged Trade Secret identified in response to Interrogatory No. 1, describe in detail how You allegedly developed such Trade Secret, including, without limitation, the circumstances under which You conceived of such Trade Secret, the identity of each Person involved in the conception, design, development, and/or use of such Trade Secret, and the nature and level of involvement of each such Person.

RESPONSE TO INTERROGATORY NO. 3:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Moog objects to this interrogatory on the grounds that it is overbroad and unduly burdensome. Moog's trade secrets at issue in this case consist of millions of files developed over decades. It is unduly burdensome for Moog to describe how and by whom each and every file was developed.

Moog objects to this interrogatory on the grounds that it is premature given the volume of Moog's trade secrets at issue in this case.

Moog objects to this interrogatory on the grounds that it is vague, ambiguous, and compound.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows:

Moog's base flight control software is called Platform. Platform is in essence the "operating system" that Moog's flight control computers use, similar to Windows or Mac OS for a standard home computer. On top of the base operating system, applications specific to the particular aircraft involved are built and sit on top of the Platform base operating system to tailor its functionality to the particular aircraft. This is akin to downloading a program or application and running it on a Windows or Mac OS operating system on a standard computer. The particular application provides a specific use, but the underlying operating system allows the entire system and machine to work.

Over the past 15 years, Moog has developed three major branches of the Platform base flight control operating system software: one for commercial aircrafts, one for military use (called "eRTOS"), and one for motor applications (called "AMP").

Platform is the generic name for the first iteration used on all commercial programs. Platform is being used in many widespread and common commercial airplanes today, including aircrafts such as 747, G280, G650, and C919. Some of Moog's project-specific software applications for military use, which sit on top of the eRTOS base software, are titled "Bell V280," "TERN," and sensitive Government Program labeled for purposes herein as "Sensitive Government Program 1." Some of Moog's project-specific software programs for motor applications, which sit on top of the AMP base software (also referred to as MMCU in later instantiations), are called "Sensitive Government Program 2," MQ-25, and Sikorsky FARA. Mike Hunter and Todd Schmidt were involved in the development and construction of the Platform base software for commercial programs. Hunter and Schmidt were the managers of the programs that created eRTOS, AMP, and the project-specific applications related to eRTOS and AMP.

Gonzalo Rey (former Director of Engineering and Chief Technology Officer) and Sathya Achar (former Engineering Technical Fellow) were the first two Moog employees to sponsor and oversee the development of Moog Platform base software beginning in 2007. Because they are in essence the architects behind the Platform base software, Messrs. Rey and Achar are the individuals with the most institutional and technical knowledge regarding the software, as well as its relationship with project-specific applications which sit on top of the base software. Messrs. Rey and Achar are intimately familiar with the Platform software code, as well as its testing and certification processes and methods.

Robert Alin Pilkington (former Senior Staff Engineer) was the lead architect on the second iteration of the Platform base software for military purposes, eRTOS. Mr. Pilkington reported directly to Hunter from 2016 until the date he departed Moog. Misook Kim and Eric Chung were software design engineers who worked under Mr. Pilkington. Ms. Kim and Mr. Chung worked on eRTOS, as well as "Sensitive Government Program 2."

A list of the individuals involved in the development, testing, and certification of the Platform software and its project-specific applications, is listed as follows:

Pursuant to Federal Rule of Civil Procedure 33(d), Moog will produce on or before April 27, 2022 documents sufficient to show the identities of employees who were involved in the development, testing, and certification of Platform, eRTOS, AMP, and each of Moog's flight control applications relevant to this case, pursuant to an agreed upon Stipulated Protective Order,

Moog incorporates by reference to this interrogatory response the statements set forth in the Complaint, its Motion for Preliminary Injunction, and the Declarations of Michael Hunter, Todd Schmidt, and Jorge Lopez filed concurrently therewith.

///

///

///

INTERROGATORY NO. 4:

For each alleged Trade Secret identified in response to Interrogatory No. 1, identify all locations, both physical and electronic, at which any copy of the alleged Trade Secret was stored, and the dates during which they were stored at the identified locations.

RESPONSE TO INTERROGATORY NO. 4:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Moog objects to this interrogatory on the grounds that it is overbroad and unduly burdensome. Moog's trade secrets at issue in this case consist of millions of files developed over decades. This interrogatory has no time limitation. It is unduly burdensome for Moog to identify the historical location of any copy of its files over the time period of decades.

Moog objects to this interrogatory on the grounds that it is premature given the volume of Moog's trade secrets at issue in this case.

Moog objects to this interrogatory on the grounds that it seeks information outside of Moog's possession, custody or control. For example, Moog cannot identify each time over the period of decades its source code has been copied by an employee onto a personal device. Further, Moog cannot identify the location of its original files to the extent they are deleted, manipulated, or altered, as transpired through the acts set forth in Moog's Complaint.

Moog objects to this interrogatory on the grounds that it is vague, ambiguous, and compound.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows:

Moog's trade secrets at issue in this case are housed on servers located in East Aurora, New York, as well as on the laptop computers of Moog employees with the required credentials as needed to work on projects relating to those trade secrets.

Certain Moog employees who have the required credentials (as discussed further below in response to Interrogatory No. 5), can access through the secured Moog network the Subversion repository which houses Moog's software database (including its source code and SEPG checklist repository). Moog employees with required credentials can access Subversion directly through the Moog network while on Moog premises or remotely through dual-factor authentication VPN.

As described in the Declaration of Bruce W. Pixley, Kim copied Moog data on at least November 17, 2021 and December 15, 2021. As described here, Pilkington copied Moog data on at least October 27, 2021 and November 12, 2021. Moog incorporates by reference its response to Interrogatory No. 2 above.

Pursuant to Federal Rule of Civil Procedure 33(d), Moog will produce on or before April 27, 2022 documents sufficient to show the various dates and times from which Defendants made copies of Moog's trade secrets at issue in this case, pursuant to an agreed upon Stipulated Protective Order.

Moog incorporates by reference to this interrogatory response the statements set forth in the Complaint, its Motion for Preliminary Injunction, and the Declarations of Ian Bagnald, Michael Hunter, Todd Schmidt, and Jorge Lopez filed concurrently therewith.

///

///

///

INTERROGATORY NO. 5:

For each alleged Trade Secret identified in response to Interrogatory No. 1, describe all actions You have taken to safeguard the confidentiality or secrecy of each such alleged Trade Secret.

RESPONSE TO INTERROGATORY NO. 5:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows:

The Platform software itself is designed to prevent hacking or reverse engineering. It cannot be reverse engineered from an aircraft computer that the software is used on. It is password protected and Moog provides the source code to partners in only very limited circumstances. The software is uploaded onto Moog electronics at Moog facilities.

Further, many Moog employees are required to sign Moog internal proprietary information agreements, as well as third party proprietary information agreements when working on certain project-specific applications.

Every new Moog hire (including any software engineer) is required to review the then-current Moog employee handbook and acknowledge the requirements therein in writing, either through a signed paper form or an electronic acknowledgment.

Moog has several security measures to safeguard its proprietary and confidential information. Moog has controlled access into its buildings. All employees go through security screening and background check before being hired.

Moog has a robust written policy regarding its intellectual property, and its confidential, proprietary, and trade secret information. This written policy is made available to every Moog employee, including all software engineers. This written policy, among other things, defines Moog's proprietary and trade secret information, provides strict protocols for storing, designating, and transmitting such information, and prevents any third party disclosure of such information.

Moog also requires all employees to complete a training regarding company "trade secrets" and other proprietary information, which confirms the contents of Moog's written IP policy.

Platform, including all attendant project-specific software, is housed on a secure server at Moog's East Aurora, New York offices. Not all employees at Moog have access to the software database.

Access to the software database is generally on a "need to know" basis that must be approved by the lead on the software program. For example, an employee can work on a software program but not be given access to the software database if the program lead determines that employee does not require access to the software database. Certain individuals in administrative or managerial roles, such as Pilkington (software manager) and Kim (one of four Subversion administrators), are granted broader access to Moog flight control artifacts.

In order to have access to Platform and related project-specific software, a Moog employee would need specific access to Moog's general network, then a separate set of credentials to Moog's software database. In total, the employee would need five separate approvals to access the Platform software (Moog employee, building access, network access, server access, project access).

The most confidential and proprietary information related to Platform and related project-specific applications, and the types of information that Moog always treats as internal trade secrets which are never disclosed to other parties, are: 1) the underlying source code for each program; and 2) certain documents and checklists prepared by Moog's Software Engineering Process Group ("SEPG"), which contain processes to ensure that the software is being developed in a manner to meet certification requirements by the FAA and other similar authorities around the world. The SEPG documents have been optimized over 20 years of working with aviation authorities around the world. Many companies hire Moog for software development specifically because Moog knows how to efficiently create and certify software with the world's various aviation authorities.

Regarding Moog's source code for its programs, every flight software source code file contains restrictive language similar to the following: "MOOG PROPRIETARY and CONFIDENTIAL INFORMATION; This technical Data/Drawing/Document contains information that is proprietary to, and is the express property of Moog Inc., or Moog Inc. subsidiaries except as expressly granted by contract or by operation of law and is restricted to use by only Moog employees and other persons authorized in writing by Moog or as expressly granted by contract or by operation of law. No portion of this Data/Drawing/Document shall be reproduced or disclosed or copied or furnished in whole or in part to others or used by others for any purpose whatsoever except as specifically authorized in writing by Moog Inc. or Moog Inc. subsidiary."

In the two instances where Moog has disclosed its flight control source code to third parties, Moog has provided its source code under strict non-disclosure and confidentiality obligations for the receiving party. Further, in both of these instances, the customer was also designing source code in tandem with Moog for the same application.

Pursuant to Federal Rule of Civil Procedure 33(d), Moog will produce on or before April 27, 2022 documents showing the efforts taken to safeguard the confidentiality of its trade secrets at issue in this case during the relevant time periods including, but not limited to, its employee handbooks, IP policies, trade secret trainings, security policies, and agreements signed by former Moog employees/contractors who now work at Skyryse, pursuant to an agreed upon Stipulated Protective Order.

Moog incorporates by reference to this interrogatory response the statements set forth in the Complaint, its Motion for Preliminary Injunction, and the Declaration of Michael Hunter filed concurrently therewith.

INTERROGATORY NO. 6:

For each alleged Trade Secret identified in response to Interrogatory No. 1, identify and describe in detail how You were harmed by the alleged misappropriation, including when.

RESPONSE TO INTERROGATORY NO. 6:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Moog objects to this interrogatory on the grounds that it is premature and seeks expert testimony. Discovery is ongoing, specifically regarding Moog's harm based on Defendant's use of Moog's trade secrets.

Moog objects to this interrogatory to the extent it seeks information outside the scope of Moog's Motion for Preliminary Injunction and/or the Stipulation Re: Expedited Discovery (ECF 33, 36). Specifically, any harm or damages faced by Moog outside the scope of the irreparable harm it has suffered in connection with its Motion for Preliminary Injunction are outside the scope of these expedited discovery proceedings.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows:

The data copied by Ms. Kim and Mr. Pilkington, and possession thereof by Skyryse, presents substantial and irreparable harm to Moog.

Unmanned helicopter aviation, which Moog and Skyryse are both pursuing, is a new market. There is no established market and no industry leader yet. About 20 companies, including Moog and Skyryse, have entered the market and are rushing to become the market leader. Skyryse's access to Moog's flight control software and related data, taken by Kim and Pilkington, provides a substantial advantage, potentially saving tens of millions of dollars and several years of work in developing that software from scratch. Even the ability to reference the materials is valuable, because it represents a complete compendium of Moog's solutions to various programming issues inherent in flight control software. Moog has invested about 5 years of research and development into unmanned helicopters and 15 years in developing the Platform software. This software takes many years to build, test, and certify.

There is generally a high barrier to entry in the flight control software market. Companies that have an established, tested, and proven software and have successfully delivered on contracts before have a huge advantage in securing contracts from the government and other third parties. Platform provides Moog with that competitive advantage. Contracting parties understand that because of Moog's Platform software, it will be faster and less expensive to tailor its flight control software to a particular aircraft because the substantial foundation has already been built. Other companies would have to pay two to three times what Moog does because Moog has an established flight control operating system software. As a result, Moog wins many of the flight control projects that it bids on.

One of the notable programs copied by Ms. Kim is the commercial program G280. This program contains all of the information and models to develop aircraft level control laws, surface level control laws, redundancy management, safety-critical architecture, high-availability system, full fly-by-wire control on 2.5 axis, back-up architecture, and all the detail necessary to derive the source code. Skyryse is now pursuing flight control systems for aircraft. The data from the G280 project is applicable to what Skyryse is pursuing and would be extremely valuable to Skyryse and would save it tremendous time, money, effort, and resources in having to build these programs from scratch.

If a third party was able to obtain the entire code and underlying data to Moog's Platform software, a large barrier to entry would be removed. Ms. Kim essentially copied almost every piece of data related to Moog's platforms for flight control software and some applications that Moog has worked on over the past 15 years. Further, based on the limited information available to Moog, Mr. Pilkington copied all or substantially all design data and source code for eRTOS, three project-specific applications, and various other flight control software tools. It is impossible to quantify the value to Moog of the amount of monetary investment, software engineering hours, and other resources that have gone into developing, testing, and certifying all of these programs and applications.

Further, by gaining access to Moog's Platform software, a third party could get access to perform software upgrades. A third party would not be able to pull information from an airplane box that has used the Platform software in order to re-program it unless it has access to Moog's software. Right now, only Moog can re-install or service an upgraded equipment or product which uses the Platform software. Re-programming an airplane computer has several security concerns. Moreover, it potentially allows third parties to take over performing work for Moog clients that currently only Moog can perform.

There are also substantial security, goodwill, and reputational issues posed by Ms. Kim and Mr. Pilkington's copying of Moog's proprietary and confidential software and related data. Under almost every contract that Moog enters into for flight software development, there is a requirement that Moog notify its customers if certain proprietary or confidential data was copied or stolen. Moog is now required to notify its military customers of the data theft at issue, including the US Government. Moog has never had to notify the US Government of anything close to the type of data breach presented by Ms. Kim's and Mr. Pilkington's actions.

Moog's required disclosure will inevitably cause harm to Moog's reputation and goodwill in the industry. Data and information security is of paramount concern in this industry, especially with the US Government. Moog has historically been regarded as excellent and trustworthy in terms of data security and confidentiality. Any notion that Moog is unsafe with its customers' data will likely bring reputational damage and may impair Moog's ability to obtain future contracts.

Moog is being harmed by the simple nature that millions of its confidential and trade secret files have been copied and taken by its former employees and current employees of its competitor, Skyryse.

Pursuant to Federal Rule of Civil Procedure 33(d), Moog will produce on or before April 27, 2022 documents sufficient to show the total number of employee hours charged and factory cost based on charged hours for Platform, eRTOS, AMP, and each of Moog's flight control applications, pursuant to an agreed upon Stipulated Protective Order.

Moog incorporates by reference to this interrogatory response the statements set forth in the Complaint, its Motion for Preliminary Injunction, and the Declaration of Michael Hunter filed concurrently therewith.

INTERROGATORY NO. 7:

For each alleged Trade Secret identified in response to Interrogatory No. 1, identify the alleged independent economic value each alleged Trade Secret has derived from not being publicly known, and include in the response the factual and legal bases underlying the calculation of this alleged value.

RESPONSE TO INTERROGATORY NO. 7:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Moog objects to this interrogatory on the grounds that it is premature because monetary damages are not relevant to the seeking of preliminary injunctive relief, and is a topic that will eventually be the subject of expert testimony.

Moog objects to this interrogatory on the grounds that it seeks information outside the scope of Moog’s Motion for Preliminary Injunction and/or the Stipulation Re: Expedited Discovery (ECF 33, 36). Specifically, Moog’s monetary damages are not at issue in its Motion for Preliminary Injunction.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows:

The Platform base software, and related project-specific applications, constitute very valuable, sensitive, and proprietary information to Moog.

The Platform software provides Moog a huge competitive advantage in the marketplace. Platform allows Moog to be a front-runner in obtaining bids from commercial or military parties. Moog's costs are lower and its schedule time is faster due to this Platform software. Moog can have a product in the lab and flying faster than its competitors due to this Platform software.

The three iterations of the Platform base software (commercial, military, motors) took 15 years in total to develop. Building the initial iteration of the Platform software required 25 software engineers over a period of two to three years.

On top of the multiple years it took to build Platform, the testing requirements for flight control software are extremely vigorous and costly. Before any flight control software is approved by the Federal Aviation Administration ("FAA") or similar governing bodies around the world, it must be vigorously tested and certified. Different types of testing and analyses are required. It takes twice as many engineers to test and certify flight software than it does to create it. Testing and certification generally constitutes two-thirds of Moog's total cost to build flight software.

Moog has invested approximately $30 million in building, testing, and certifying its Platform software over the past 15 years. About $11 million of engineering hours were used to develop the original Platform base software for commercial use. About $5 million of software engineering hours were used to develop the eRTOS software for military use. About $14 million of engineering hours were used to develop the AMP software package. Moog has invested approximately $100 million in building, testing, and certifying its aircraft project-specific software applications that sit on top of the Platform software. Moog has also invested over $30 million to date into the market of unmanned helicopters.

If another party was able to obtain Moog's Platform base software, or any component of it, it would provide a huge competitive advantage to that company.

If a third party had possession of Moog's Platform software, including its underlying code, testing, and certification requirements, the third party company could easily "click and build" a project specific software on top of the base software in a short amount of time. The only additional item the party would need to build a flight control computer would be an electronic flight computer and the requirements to start building the flight control application.

It is impossible to quantify the amount of monetary investment, engineering hours, and other resources that have gone into developing, testing, and certifying all of these projects and applications. This information is truly priceless and represents the highest level of intelligence and wisdom of Moog's smartest architects of the past 15-20 years. It is from this and similar technology that Moog generates $1 billion annually in revenue.

Part of what makes Moog unique and competitive in the marketplace is that it can design entire systems for aircraft flight controls (i.e., software, electrical hardware, and mechanical hardware) and integrate all aspects together in-house. Most other competitors can only do one or the other. Moog builds software and hardware systems safely through the use of architectural diagrams. Ms. Kim copied Moog's systems and/or software architectural diagrams for 8-9 project specific applications. Further, based on the limited information available to Moog, Mr. Pilkington copied all or substantially all design data and source code for eRTOS, three project-specific applications, and various other flight control software tools. This information in the hands of Skyryse removes a large barrier to entry and saves Skyryse tens of millions of dollars and several years of work and represents a vast amount of experience learned by Moog engineers.

Pursuant to Federal Rule of Civil Procedure 33(d), Moog will produce on or before April 27, 2022 documents sufficient to show the total number of employee hours charged and factory cost based on charged hours for Platform, eRTOS, AMP, and each of Moog's flight control applications, pursuant to an agreed upon Stipulated Protective Order. Moog will also produce on or before April 27, 2022 documents sufficient to show the identity of employees who were involved in the development, testing, and certification of Platform, eRTOS, AMP, and each of Moog's flight control applications, pursuant to an agreed upon Stipulated Protective Order.

Moog incorporates by reference to this interrogatory response the statements set forth in the Complaint, its Motion for Preliminary Injunction, and the Declarations of Michael Hunter, Todd Schmidt, and Jorge Lopez filed concurrently therewith.

INTERROGATORY NO. 8:

For each alleged Trade Secret identified in response to Interrogatory No. 1, identify when (if ever), how, and to whom Moog disclosed, accessed, or otherwise provided to anyone (including each person who has left Moog in the last 5 years) any of the alleged Trade Secrets and describe the extent and circumstances of the disclosure.

RESPONSE TO INTERROGATORY NO. 8:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Moog objects to this interrogatory on the grounds that it is overbroad and unduly burdensome. Moog's trade secrets at issue in this case consist of millions of files developed over decades. This interrogatory has no time limitation. It is unduly burdensome for Moog to identify each and every historical access to Moog's trade secrets.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows:

Pursuant to Federal Rule of Civil Procedure 33(d), Moog will produce on or before April 27, 2022 documents sufficient to identify the Moog employees who have had access to Moog's trade secrets at issue in this case, and the manner and timing of such access, pursuant to an agreed upon Stipulated Protective Order. Moog will also produce documents sufficient to identify the other limited circumstances under which Moog has provided any access to the trade secrets at issue in this case to third parties, pursuant to an agreed upon Stipulated Protective Order.

INTERROGATORY NO. 9:

For each alleged Trade Secret identified in response to Interrogatory No. 1, identify and describe how each Defendant allegedly improperly used or disclosed each alleged Trade Secret.

RESPONSE TO INTERROGATORY NO. 9:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Moog objects to this interrogatory on the grounds that it is premature. Discovery is ongoing regarding the nature and extent of use or disclosure of Moog's trade secrets by Defendant.

Moog objects to this interrogatory on the grounds that it seeks information outside the possession, custody or control of Moog and uniquely in the possession, custody or control of the defendants in this case, including Defendant.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows: Moog incorporates by reference its response to Interrogatory No. 2 above. Further, regarding Skyryse's acquisition or use of Moog's trade secrets, Skyryse has acknowledged (including in a letter dated April 4, 2022), that Misook Kim's Skyryse-issued laptop received Moog data from one or more of the devices that was used in the data copying on November 19, 2022. Skyryse has further acknowledged that over 11,000 identical Moog files were discovered on Robert Alin Pilkington's Skyryse-issued laptop. Moog's investigation is ongoing, which will include an analysis of the 25 electronic devices and additional data turned over by Defendants to iDS.

INTERROGATORY NO. 10:

Identify each Former Moog Employee and describe in detail all facts regarding the departure of each Former Moog Employee, including the date on which such Former Moog Employee notified You of their intent to leave, the Former Moog Employee's last date of employment, the time and content of any "exit interview," and whether You requested or required the Former Moog Employee to leave their employment earlier than the Former Moog Employee offered or requested to continue working.

RESPONSE TO INTERROGATORY NO. 10:

Moog incorporates by reference the Preliminary Statement and General Objections as though fully set forth herein.

Moog objects to this interrogatory on the grounds that it is vague, ambiguous, and compound.

Subject to, and without waiving any of the foregoing objections, Moog responds as follows: Pursuant to Federal Rule of Civil Procedure 33(d), on or before April 27, 2022, Moog will produce documents regarding the departure of each former Moog employee who is now employed by Skyryse, pursuant to an agreed upon Stipulated Protective Order.

Dated: April 13, 2022

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
Attorneys for Plaintiff Moog Inc.

By /s/ Rena Andoh
Rena Andoh
Travis Anderson (pro hac vice)
Kazim A. Naqvi (pro hac vice)
30 Rockefeller Plaza
New York, New York 10112
Telephone: (212) 653-8700

HODGSON RUSS LLP
Attorneys for Plaintiff Moog Inc.

By /s/ Robert J. Fluskey Jr.
Robert J. Fluskey Jr.
Melissa N. Subjeck
Pauline T. Muto
The Guaranty Building
140 Pearl Street
Buffalo, New York 14202
Telephone: (716) 856-4000

VERIFICATION

I have read the foregoing **MOOG INC.'S RESPONSES TO DEFENDANT SKYRYSE, INC.'S FIRST SET OF (EXPEDITED) INTERROGATORIES** and know its contents.

I, Michael Hunter, am the Software Senior Manager of Moog Inc., a party to this action, and am authorized to make this verification for and on its behalf, and I make this verification for that reason. I am informed and believe, and on that ground allege, that the matters stated in the foregoing document are true based on my personal knowledge, inspection of the books and records of Moog, and conversations with other employees of Moog.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on April 13, 2022.

MICHAEL HUNTER

PROOF OF SERVICE

Moog Inc. v Skyryse, Inc. et al.
1:22-cv-00187

At the time of service, I was over 18 years of age and **not a party to this action**. I am employed in the County of Los Angeles, State of California. My business address is 1901 Avenue of the Stars, Suite 1600, Los Angeles, CA 90067-6055.

On April 13, 2022, I served true copies of the following document(s) described as **MOOG INC.'S RESPONSES TO DEFENDANT SKYRYSE, INC.'S FIRST SET OF (EXPEDITED) INTERROGATORIES**

on the interested parties in this action as follows:

SEE ATTACHED SERVICE LIST

BY E-MAIL OR ELECTRONIC TRANSMISSION: I caused a copy of the document(s) to be sent from e-mail address knaqvi@sheppardmullin.com to the persons at the e-mail addresses listed in the Service List. I did not receive, within a reasonable time after the transmission, any electronic message or other indication that the transmission was unsuccessful.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that I am employed in the office of a member of the bar of this Court at whose direction the service was made.

Executed on April 13, 2022, at Los Angeles, California.

/s/ Kazim A. Naqvi
Kazim A. Naqvi

SERVICE LIST

HARRIS BEACH PLLC
Terrance P. Flynn
726 Exchange Street, Suite 1000
Buffalo, New York 14210
(716) 200-5050
tflynn@harrisbeach.com

Attorneys for Defendant SKYRYSE, INC.

GIBSON, DUNN & CRUTCHER LLP
Josh Krevitt, Esq.
Kate Dominguez, Esq.
Ilissa Samplin, Esq.
Angelique Kaounis, Esq.
Justine Goeke, Esq.
Michael Polka, Esq.
200 Park Avenue
New York, NY 10166
(212) 351-2338
JKrevitt@gibsondunn.com
KDominguez@gibsondunn.com
ISamplin@gibsondunn.com
AKaounis@gibsondunn.com
JGoeke@gibsondunn.com
MPolka@gibsondunn.com
Skyryse-TradeSecretsLitigation@gibsondunn.com

Attorneys for Defendant SKYRYSE, INC.

LOCKE LORD
Rory S. Miller, Esq.
Mitchell Popham, Esq.
Will Mullen, Esq.
Joseph Froehlich, Esq.
300. S. Grand Avenue, Suite 2600
Los Angeles, CA 90071
(213) 485-1500
Rory.Miller@lockelord.com
MPopham@lockelord.com
William.Mullen@lockelord.com
JFroehlich@lockelord.com

Attorneys for Defendants
ROBERT ALIN PILKINGTON and
MISOOK KIM